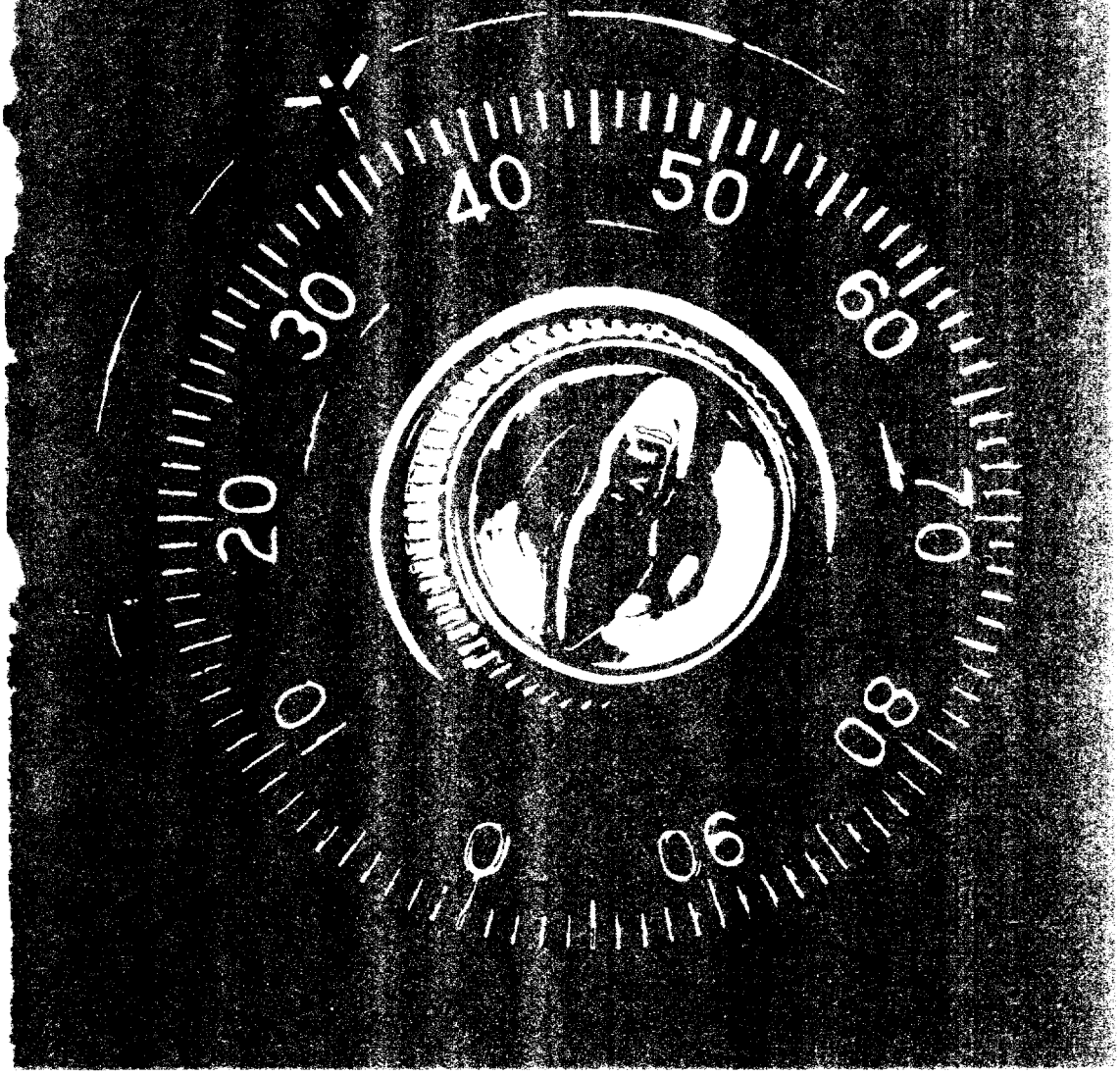
DOE material
used at NARS
Conference
14-15 Sept 1982

DOE review
completed.

Approved For Release 2007/11/01 : CIA-RDP85B00236R000100050001-8

What You Should Know About

DOE SECURITY



What You Should Know About
DOE SECURITY

Prepared By The
Office Of Safeguards & Security
Washington, D.C.

This pamphlet provides information regarding several fundamental aspects of the DOE security orders and is published to assist and guide personnel in complying with these orders. The reading of this pamphlet, however, IS NO SUBSTITUTE for a review of the Department of Energy security issuances which have been made available to your supervisor. The security issuances pertaining to your activities must be reviewed prior to your handling of classified information.

Supervisory personnel at all management levels, with appropriate guidance from the responsible security office, must assure that each employee under their supervision is kept fully informed as to his security responsibilities.

February, 1979 (Rev.)

I. RESPONSIBILITIES

Security is an individual responsibility. Each individual is personally responsible for the security of classified information entrusted to his care.

Your security office will assist you in the discharge of your security responsibilities. Questions, oral or written, may be directed to that office at any time.

II. TYPES OF INFORMATION

The Department of Energy (DOE) originates and receives three types of information:

CLASSIFIED INFORMATION[1]
PRIVILEGED AND PROPRIETARY INFORMATION
UNCLASSIFIED INFORMATION

A. CLASSIFIED INFORMATION

The term "Classified Information" includes three categories:

(1) Restricted Data, as defined in the Atomic Energy Act of 1954, is all data concerning (a) design, manufacture, or utilization of atomic weapons; (b) the production of special nuclear material; or (c) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954.

[1]In DOE the use of the term, National Security Information, does *not* include Restricted Data or Formerly Restricted Data. Its use in this pamphlet does *not* include RD or FRD.

(2) Formerly Restricted Data is data which has been transclassified from the Restricted Data category and relates primarily to the military utilization of atomic weapons (see V.B. below).

(3) National Security Information is information which requires safeguarding in the interest of the national security. (Its use in the DOE does not include RD or FRD).

Restricted Data, Formerly Restricted Data and National Security Information may be classified as:

TOP SECRET (TS)
SECRET (S)
CONFIDENTIAL (C)

The significance of these classification categories which reflect the varying degrees of sensitivity of information to the national security is fully explained in DOE Order 5650.2. For the purpose of this pamphlet, the classification may be briefly described as follows:

TOP SECRET: is classified information or material which requires the highest degree of protection and the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

SECRET: is classified information or material which requires a substantial degree of protection and the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

CONFIDENTIAL: is classified information or material which requires protection and the unauthorized disclosure of which could reasonbly be expected to cause identifiable damage to the national security.

In the assignment of a classification, it is necessary that the authorized classifier determine whether the information is Restricted Data, Formerly Restricted Data or National Security Information. On documents, this distinction is indicated by the use of the Restricted Data, Formerly Restricted Data or the National Security Information stamp, as appropriate, on the cover sheet, title page, and the first page of a document. The necessity for indicating the distinction between Restricted Data, Formerly Restricted Data, and National Security Information will become apparent after reading paragraphs III.B1., 2., and 3. below.

The Office of Classification, DOE, will be glad to assist persons having classification questions. That Office will furnish guidance as to the level of

classification assigned to specific items or areas of information and as to whether such information is Restricted Data (RD), Formerly Restricted Data (FRD), National Security Information (NSI), or unclassified.

B. PRIVILEGED AND PROPRIETARY INFORMATION

The Department of Energy recognizes the existence of information, not affecting the national security, which is of a privileged or proprietary nature and which should receive limited dissemination as is customary under standard industrial, professional, academic, and Government practices. Privileged and proprietary information is not classified and is designated by the DOE with the marking "Official Use Only" (OUO). DOE contractors may mark documents which they originate in this category with terms indicating that they contain privileged or proprietary information, such as "Private," "Company Confidential," and "Business Confidential."

There is a State Department marking for privileged information which is "Limited Official Use" (LOU). LOU must be stored, as a minimum, in a combinated bar lock security container. OUO must be stored in such a manner not to arouse the curiosity of people who do not have the "need-to-know." Both OUO and LOU must be destroyed as if they were classified information to preserve the proprietary and privileged interest.

C. UNCLASSIFIED INFORMATION

Information which does not affect the national security and which does not fall within Sections A and B above is considered unclassified and requires no form of security protection.

A document may bear a marking indicating that it is "Unclassified" if it is essential to convey to any person who has access to the document that it does not require classification or Official Use Only handling. This marking may be placed on a document at the time of preparation, after it has been declassified or after it has been removed from the "Official Use Only" status.

III. ASSURANCES TO BE OBTAINED BEFORE GRANTING ACCESS

A. GENERAL

Security regulations require that a person have the prescribed access authorization[2] and the "need-to-know" prior to being afforded access to classified information.

---

[2]Access authorization is the term for security clearance used in the DOE Orders. In this pamphlet the terms are used interchangeably.

B. ACCESS AUTHORIZATION

1. Background

Pursuant to the Atomic Energy Act of 1954, as amended, the DOE controls the dissemination of Restricted Data and Formerly Restricted Data in a manner designed to assure the common defense and security. National Security Information is controlled in accordance with applicable Federal statutes and Presidential Executive Orders.

No person may have access to classified information unless he or she has been granted an access authorization. The DOE grants four types of access authorizations. (1) A "Q" access authorization (or "Q" clearance) permits a person to be eligible for all levels (TS, S and C) of RD, FRD and NSI; (2) An "L" access authorization (or "L" clearance) permits a person to be eligible for C RD and S FRD and NSI; (3) A "TS" access authorization (or "TS" clearance) permits a person to be eligible for TS, S and C FRD and NSI; (4) An "S" access authorization (or "S" clearance) permits a person to be eligible for S and C FRD and NSI. NOTE: TS and S clearances do *not* permit eligibility for any level of RD.

Responsible Heads of Offices in the DOE (or their designees) determine the scope and highest classification of information to which the cleared person is to be granted access. The determination by the Head of an Office is in accordance with the compartmentalization policy of the DOE, which states that authorized personnel shall be provided with that information which they need for the performance of their duties. This is commonly called the "need-to-know" policy. It is the policy of the DOE generally to segregate information on very sensitive information, such as production rates and stockpile information. Prior to access to this type of information, specific authority is required. (Intelligence, cryptographic and other information so designated by Statute, Executive Orders, International Agreements, etc.)

2. Prescribed Access Authorization for Access to Restricted Data

As a general rule an individual must have a "Q" access authorization before being afforded access to Restricted Data. Three exceptions to this rule are outlined below:

a. *Access to Confidential Restricted Data.* When personnel require access to Restricted Data classified no higher than Confidential, an "L" access authorization is sufficient.

b. *Access by the Department of Defense.* Dissemination of Restricted Data to personnel of the DOD or of its contractors or members of the Armed Forces by employees of the DOE or of its contractors may be permitted upon proper certification by, or in the name of, designated DOD personnel or Armed Forces personnel, of the intended recipient's access authorization and "need-to-know". Employees of other Federal

agencies appropriately cleared by the DOE may similarly disseminate Restricted Data to personnel of the DOD.

c. *Access by the National Aeronautics and Space Administration.* Dissemination of Restricted Data to personnel of the NASA or of its contractors by employees of the DOE or of its contractors may be permitted upon proper certification by, or in the name of, designated NASA personnel, of the intended recipient's access authorization and "need-to-know," but only where the Restricted Data is concerned with aeronautical and space activities. When the Restricted Data to be disseminated involves matters other than aeronautical and space activities, a "Q" access authorization is required for NASA and NASA contractor employees. Employees of other Federal agencies appropriately cleared by the DOE may similarly disseminate Restricted Data to NASA.

The procedures under which Restricted Data may be disseminated to DOE and NASA are more fully explained in DOE Orders 5631.5 and 5635.2.

3. Prescribed Access Authorization for Classified Information Other Than Restricted Data

Any access authorization granted by the DOE permits a person to be eligible for the levels of classification of Formerly Restricted Data and National Security Information appropriate to his or her access authorization. When access is required by a DOE or contractor employee to such information in the custody of another government agency, arrangements should be made through the responsible security offices for such access.

Conversely, a person from another government agency or its contractors may be afforded access to Formerly Restricted Data and other National Security Information in the custody of the DOE after proper assurance has been obtained that he has an access authorization for the same or higher classification than that assigned to the information he desires. Such assurance should be obtained through the responsible security office.

4. Access Authorization Not Required for Privileged or Proprietary Information

Since privileged or proprietary information is unclassified there is no requirement for any type of access authorization.

C. NEED-TO-KNOW ASSURANCE

Access to classified information may be afforded only to those cleared individuals who need the information in the performance of their official duties. Privileged or proprietary information may be transmitted to individuals, cleared or uncleared, who need the information for official purposes.

D. PROTECTION OF CLASSIFIED MATTER IN STORAGE

Limited Official Use, Confidential, Secret, and Top Secret documents shall be stored in approved repositories whenever the room in which the material is being used is unattended. Official Use Only must be stored in a manner which will not reveal the contents to personnel who do not have the "need-to-know." Applicable instructions governing types of containers and protection requirements appear in DOE Order 5632.1.

E. HOW TO OBTAIN INFORMATION ON THE ABOVE ASSURANCES

Your responsible security office can supply you with the information on prescribed personnel access authorizations and approved storage facilities. With respect to the "need-to-know," the determination must be made by you or by your supervisor or higher authority.

IV. BADGES

DOE issues the following types of badges:

1. Picture badges with a "Q", "L", "TS" or "S" on the badge which identify the holder and the type of access authorization granted. Similar badges, without picture, are issued when employees have forgotten or lost their picture badge. These badges, with or without pictures, have a green background.

2. Picture badges without an access authorization designation who do not require a clearance. A badge, with an "E" instead of a picture is issued when the picture badge has been forgotten or lost. These badges, with or without pictures, have a black background.

3. Picture badges with a "Q", "L", "TS", or "S" on the badge with a green background and red vertical lines which identify the holder as a contractor employee.

4. Visitors, holding access authorization, and issued a green background badge, without picture, reflecting the type of access authorization granted. (Visitors holding access authorization do not require escort in security areas.)

5. Visitors, not holding an access authorization, will be issued a "V" badge with a black background without a picture. (Visitors not holding access authorization *will be* escorted in security areas by DOE *security cleared* individuals.)

V. CLASSIFICATION PROCEDURES

A. GENERAL

The listing of the types of information in the DOE and the definitions of TOP SECRET, SECRET, and CONFIDENTIAL as shown in II above are not intended to be guides to the classification of individual documents. The Office in the DOE which sponsored your access authorization or the Office of Classification as noted above should be contacted for appropriate guidance as to your classification problems. Remember, however, that only repeated reference to classification guides can lead to skill in proper classification.

The definitions of the three classifications should indicate to you, however, what could happen in the event of improper classification or failure to observe security requirements. Failure to properly classify a document may cause you to be a contributing party to an unauthorized disclosure and may subject you to penalties attached thereto.

Authority to classify may be delegated to you, if appropriate, in writing in accordance with the provision of DOE Order 5650.2. If your organization has not been delegated classification authority, you may contact the Office of Classification if you feel that you require such authority. Requests for designation of persons who are to authenticate[3] Top Secret documents must be submitted in writing to the Director, Office of Classification, in Washington, with a copy to the Director, Office of Safeguards and Security. All delegations are subject to approval and cancellation by the DOE.

Procedures for obtaining declassification authority are outlined in DOE Order 5650.1.

Classified documents should be continuously reviewed for purposes of declassification or reduction in classification (downgrading).

B. TRANSCLASSIFICATION

Transclassification is the removal of information or materials from the category of Restricted Data and transferral of them either (1) to the category of Formerly Restricted Data, pursuant to the provisions of Section 142(d) of the Atomic Energy Act of 1954, and subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data, or (2) to National Security Information pursuant to Section 142(e) of the Act if it pertains to the atomic energy programs of foreign nations. Detailed instructions, including special markings to be placed on such information, are contained in DOE Order 5635.2.

---

[3] Authentication refers to the certification that a document requires a Top Secret classification.

290-023 O - 79 - 2

C. AUTOMATIC DECLASSIFICATION

Restricted Data and Formerly Restricted Data can only be declassified in accordance with declassification guides or guidance obtained from the Office of Classification, DOE.

With respect to National Security Information, all original classification authorities shall, at the time of original classification determination, set a specific date or event for automatic declassification of the information. The date or event shall be as early as the national security interest will permit; but in no case shall the date or event exceed six years from the date of origin of the information that is classified. In those cases where there is a need, directly related to the national security, to continue classification beyond six years, only Top Secret classification authorities may set a later date or event for automatic declassification or declassification review. Such action must be recorded on each copy.

VI. MARKING DOCUMENTS

All documents containing classified information must be marked at the top and bottom of each page with the appropriate classification. In addition, to assist recipients in their determination of the security clearance prescribed for access thereto, the Restricted Data, Formerly Restricted Data, or National Security Information marking, as appropriate, must be placed on the cover sheet and title page if the document has a cover sheet and title page, and, in all cases on the first page of each copy.

Top Secret and Secret documents must be documented by use of the following stamp:

This document consists of _____ pages

No. _____ of _____ Copies, Series _____.

All blanks must be completed with the required information. This stamp is required to be placed in the upper right hand corner of the first page of each copy.

Special authorization is required for originating and obtaining access to TOP SECRET documents. Procedural instructions for the handling of such documents are set out in DOE Order 5635.2.

Letters of transmittal bearing contents of a lower classification than that of the documents forwarded therewith must be marked at the top and bottom of each page with a classification at least equal to that of the most highly classified enclosure. The fact that the enclosures contain Restricted Data, Formerly Restricted Data, or National Security Information must also be indicated on the first page of the letter of transmittal. The "When Separated"

stamp set forth below must also be affixed on the first page to indicate the classification of the letter of transmittal when detached from the enclosure or enclosures.

When separated from enclosures, handle this document

as _____ _____
(Insert proper classification)

VII. PREPARATION FOR TRANSMISSION

A classified document prepared for transmission outside of a security area must be enclosed in two opaque envelopes. The inner envelope must be properly addressed and bear the appropriate classification marking and extra marking (Restricted Data, Formerly Restricted Data, or National Security Information marking). The outer envelope must be addressed in the ordinary manner with no indication of the classification of the contents.

Receipts must be inserted in the inner envelope if the document is Top Secret or Secret. Double envelopes are used to assure greater security to the document transmitted as well as to notify the person opening the outer envelope of the classification of the document or documents enclosed prior to access to the contents. In this way, mail room personnel are aided in delivering classified matter to properly cleared individuals.

VIII. TRANSMISSION

Top Secret documents may be transmitted between security areas only by authorized Top Secret couriers. When it is planned to transmit other classified documents via U.S. mail only Registered mail must be used for Secret. Registered, Certified, First-Class, or Postal Express mail is authorized for Confidential.

Personnel holding appropriate access authorizations (see III.B. above) may personally transport Secret and Confidential between security installations provided specific authority is obtained and requirements of DOE Order 5635.2.

Removal of classified documents from security areas under the authority prescribed by DOE Order 5635.2 is not to be interpreted as authorization to remove classified documents to private residences. Removal of classified documents to private residence is prohibited unless incidental to official travel.

DOE Order 5635.2 contains detailed instructions on transmission of classified documents outside the continental limits of the United States.

IX. OTHER SECURITY CONSIDERATIONS

A. Don't discuss classified information on the telephone, in carpools, or at office luncheons or out of security areas.

B. Determine, if in doubt, that the information contained in speeches or articles is unclassified prior to delivery or publication. To do this, transmit a written copy to the DOE Headquarters Office sponsoring your access authorization or to the Office of Classification, USDOE, Washington, DC 20545.

C. Read the security regulations for details. If additional assistance is required, contact the person who initiated the request for your clearance or the DOE security office responsible for your project.

D. Notify the responsible DOE security office regarding:

- In advance, of any contemplated travel to any Communist controlled nation;
- Arrests, charges (including charges that are dismissed) or detentions by Federal, State or other law enforcement authorities, for any violation of any Federal Law, State Law, county or municipal law, regulation or ordinance (other than traffic violations for which a fine of $30 or less was imposed) occurring during any period in which you may hold a DOE access authorization or which occurred subsequent to the completion of your personnel security forms;
- marriage subsequent to completion of your personnel security forms;
- contemplated visits to other facilities where your DOE security clearance must be verified;
- thefts or suspected thefts of government or personal property;
- actual or suspected losses or compromises of classified information;
- any contacts made by, or communications received from, representatives of communist controlled countries, wherein inquiries or requests relative to your official duties are made;
- any other situation which may constitute a threat to classified or sensitive information or to DOE facilities or personnel.

The office listed below is available to assist you:

Office of Safeguards and Security
Director, Division of Security
U.S. Department of Energy
Washington, DC 20545

Phone: (local calls) 353–5562
(I.D calls) 301–353–5562

U.S. GOVERNMENT PRINTING OFFICE : 1979 O - 290-023

Approved For Release 2007/11/01 : CIA-RDP85B00236R000100050001-8